Cassandra Crossing/ Zoom, privacy alla “cinese”

(459)—Un comunicato del CEO dell’azienda cinese esclude la crittografia end-to-end per gli account gratuiti.

Cassandra Crossing/ Zoom, privacy alla “cinese”

(459)—Un comunicato del CEO dell’azienda cinese esclude la crittografia end-to-end per gli account gratuiti.

6 giugno 2020—Chi segue Cassandra nelle sue molteplici identità sa che, essendosi addentrata nei dettagli e nei test di varie piattaforme di videoconferenza, considera Zoom qualitativamente la più performante, sia in termini qualitativi che per flessibilità d’uso, particolarmente la versione entry level a pagamento.

Confrontandandoli, software più liberi ed autogestibili come Jitsi, che è probabilmente il migliore nella sua categoria, sono molto inferiori in ambedue i settori.

Per questo, in un convegno virtualizzato e completamente pubblico come è stato l’ultimo e-privacy XXVII, Cassandra non si è fatta nessuna remora ad utilizzarlo.

Si, capita anche di usare software proprietari quando non esiste alternativa libera.

Si, quando la comunicazione è totalmente pubblica non è necessario occuparsi di privacy, visto che né dati né metadati sono rilevanti ai fini della privacy.

Quindi tenere un convegno pubblico usando Zoom e streaming live su Youtube, secondo l’opinione di Cassandra, anche per un paranoico pessimista non è certo ottimale ma è largamente accettabile.

D’altra parte molte delle obiezioni tecniche riguardo ai problemi di “privacy” di Zoom (come lo Zoombombing) erano ben poco rilevanti nella realtà, visto che si trattava di problemi dovuti ad un acefalo ed errato uso delle opzioni disponibili nel programma e dei loro default, od a bug prontamente corretti di un software ed un infrastruttura “giovane” ed in crescita esplosiva.

Tra l’altro fonti, autori, intensità e tempistica degli articoli che si sono accaniti contro Zoom apparivano, “andreottianamente”, alquanto sospetti; veniva da pensare che fossero ispirati da concorrenti che molto stavano investendo nel settore della videoconferenza, e che tra l’altro hanno un passato provatamente piuttosto “torbido” per quanto attiene la difesa della privacy dei propri utenti.

Ma i comunicati e le precisazioni degli ultimi giorni da parte del Chief Executive Officer di Zoom Eric Yuan, e le successive ulteriori “precisazioni” appaiono invece mostrare una netta deriva di Zoom verso una gestione “*alla cinese*” della privacy degli utenti.
Ma chiariamo, ancor prima di entrare nei dettagli della questione, che la gestione attuale della privacy da parte di altre superpotenze commerciali di varia democrazia non è, a ben vedere, affatto migliore (grazie Edward).

Yuan, in buona sostanza, ha comunicato la scelta (aziendale e quindi legittima) di riservare l’annunciata ed appena introdotta crittografia end-to-end ai soli clienti paganti, escludendola invece per quelli gratuiti, che usufruiranno invece della sola crittografia di canale.

Nel giustificare questa peraltro largamente discutibile scelta ha però segnato anche un grande autogol, affermando che “…per gli utenti free certamente non volevano concedere la crittografia

end-to-end in quanto volevano lavorare con l'FBI e le polizie locali nel caso qualcuno usasse Zoom per scopi"*malvagi*."

Ora, fin dai tempi della oramai "storica" richiesta di introduzione del Clipper Chip, ogni tentativo di indebolire la crittografia dei software con la giustificazione di tutelare la sicurezza dei cittadini onesti e della democrazia, è stato messo tecnicamente in discussione fino ad essere scartato.

E fin dall'inizio la comunità crittografica di tutto il mondo ha criticato e denunciato queste iniziative, fino ad arrivare a sbeffeggiare chi periodicamente propone qualcosa di simile (esportazione di solo software "debole", key escrow, backdoor di Stato ed altro).

E questa campana è ciò che si sente risuonare nell'affermazione di Yuan il quale, **considerato il paese di origine ed il tecnocontrollo sociale colà imposto e completamente realizzato**, dovrebbe stare un po' più attento alle sue dichiarazioni pubbliche, evitando se non altro di usare giustificazioni così vetuste ed abusate.

E meglio non ha fatto successivamente, come riferisce Bruce Schneier precisando che:

"*Zoom non fornisce informazioni alle autorità eccetto che in casi come l'abuso di minori, … non monitora proattivamente i suoi utenti, … non esistono backdoor che permettano a terzi di entrare in una videoconferenza senza essere visti*".

Tutte affermazioni che, con prosa molto datata, **sono davvero molto poco rassicuranti.**

Assai più grave affermare che "*…la crittografia AES256 è disponibile anche per i clienti non paganti*" poiché si tratta di un lampante tentativo di nascondere la realtà, confondendo volutamente la crittografia di canale, disponibile anche ai clienti free, con quella end-to-end, che garantisce una riservatezza molto maggiore ed è disponibile solo per i clienti paganti.

Approccio molto "cinese" (ma ahimè anche "americano", "inglese", "francese" e "russo") che è ben il caso di mettere in evidenza e sbeffeggiare anche in questa occasione.

Quindi, come precisato all'inizio, se dovete fare videoconferenze di buona qualità per un convegno, Zoom è senz'altro una ottima scelta, ma se volete farle con un livello di privacy ragionevole o se si tratta di comunicazione anche solo leggermente riservate, scartatelo, ma scartate anche tutti gli altri software di videoconferenza commerciali.

Utilizzate invece software libero come Jitsi ed i suoi simili, sobbarcandovene serenamente la configurazione, i costi di infrastruttura ed in generale tutto quello "sbattimento" che è indispensabile per tutelare i diritti civili digitali e la privacy, **tutela che nessuno, nemmeno le democrazie più o meno compiute, farà mai al posto vostro**.

By Marco A. L. Calamari on June 7, 2020.

Canonical link

Exported from Medium on August 27, 2025.